数理解析研究所講究録 1456 巻 2005 年 1-9

主係数が特異な場合の多変数多項式の解析的因数分解

岩見真希
筑波大学数理物質科学研究科*

MAKI IWAMI
GRADUATE SCHOOL OF PURE AND APPLIED SCIENCES, UNIVERSITY OF TSUKUBA

1 はじめに

代数的な諸計算を行う数式処理の基盤技術の一つに，解析的因数分解，すなわち，形式的べき級数環での因数分解がある．例えば，2 変数多項式 $x^2-u^2-u^3$ は多項式環では既約だが，形式的べき級数環では，原点で $(x+u+\frac{1}{2}u^2-\frac{1}{8}u^3+\cdots)(x-u-\frac{1}{2}u^2+\frac{1}{8}u^3-\cdots)$ と因数分解できる．これは幾何的な諸性質とも関係するもので，図 **1.** のように，代数曲線 $F_1=0$ が原点で解析的に可約，$F_2=0$ が原点で解析的に既約であることは，それぞれ原点での曲線の接線と関連づけて解釈できる．3 変数以上では局面の既約成分への分解と解釈できる．Weierstrass の予備定理により，1 つの変数に関しては多項式としてよいので，これを主変数 x とする．したがって，実際には，$\overline{K}\{\boldsymbol{u}\}[x]$ での因数分解としてよい．以下，記号とその意味は図 **2.** を参照されたい．

$$\begin{aligned} F_1 &= x^2-u^2-u^3 \\ &= (x+u+\tfrac{1}{2}u^2-\tfrac{1}{8}u^3+\cdots) \\ &\times\ (x-u-\tfrac{1}{2}u^2+\tfrac{1}{8}u^3-\cdots) \end{aligned}$$

$F_2=x^2-u^3$
既約

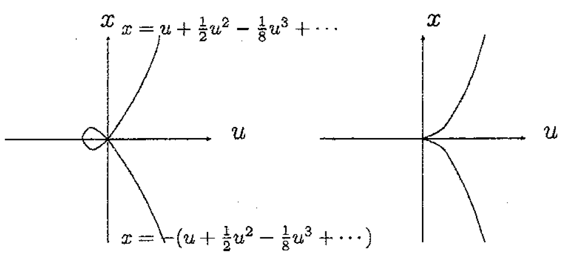


図 **1.** 2 変数解析的因数分解の例

記号	意味
x	主変数
$\boldsymbol{u}$	従変数 $u_1,\cdots,u_\ell$ の略記
$\boldsymbol{s}$	展開点 $s_1,\cdots,s_\ell$ の略記．(一般性を失うことなく $\boldsymbol{0}$ としてよい)
K	標数 0 の数体
$\overline{K}$	K の代数的閉体
$K[x,\boldsymbol{u}]$	K 上の変数 $x,\boldsymbol{u}$ の多項式環
$\overline{K}\{\boldsymbol{u}\}$	$\overline{K}$ 上の変数 $\boldsymbol{u}$ の形式的べき級数環
$\overline{K}(\theta_1,\cdots,\theta_{\tilde{d}})$	代数関数 $\theta_1,\cdots,\theta_{\tilde{d}}$ を添加した体
$\overline{K}\{(\boldsymbol{u})\}$	$\overline{K}$ 上の $\boldsymbol{u}$ の非負位数有理式の級数環

図 **2.** 記号とその意味

計算機代数でよく知られているように，Hensel の補題を利用した一般 Hensel 構成を用いて，$\overline{K}\{\boldsymbol{u}\}[x]$ での分解を行うことができる．分解した結果，一般 Hensel 構成ではそれ以上分解できない要素 $F(x,\boldsymbol{u})=f_D(\boldsymbol{u})x^D+\cdots+f_0(\boldsymbol{u})$ ただし $F(x,\boldsymbol{0})=x^D(D=\deg_x(F)\geq 2)$ または $f_D(\boldsymbol{0})=0$ (主係数特異) に帰着する．この，一般 Hensel 構成が破綻するときの分解には，拡張 Hensel 構成 [8, 9] を用いる．拡張 Hensel 構成とは，$u_i\rightarrow t^{\omega_i}u_i(i=1,\cdots,\ell)$ として従変数に関する重み付き全次数変数 t を導入し，横軸に x のべき，縦軸に t のべきをとった 2 次元 (e_x,e_t)-平面上に $F(x,t\boldsymbol{u})$ の各項に対応する点をプロットし，それらの点

*maki@math.tsukuba.ac.jp
maki@risk.tsukuba.ac.jp (2005 年 4 月より 筑波大学システム情報工学研究科)

の凸包の 1 つの下辺である Newton 線 $\mathcal{L}_{\mathrm{New}}$ 上の点に対応する項を全て足し合わせた Newton 多項式 F_{New} を，互いに素な因子の積に分解し，これらを初期因子として Hensel lifting することで F の因子を構成する方法である．本稿では，$\omega_i = 1$ $(i = 1, \cdots, \ell)$ とし，F_{New} の $\overline{K}[x, \boldsymbol{u}]$ での既約因子を初期因子として拡張 Hensel 構成で lifting する．

この場合，$F = (x^2 - u^3)^2 - u^7$ のように，Newton 多項式が $\overline{K}[x, \boldsymbol{u}]$ で $F_{\mathrm{New}} = (x^2 - u^3)^2$ と重複していて互いに素な因子の積に分解できないような F の $\overline{K}\{\boldsymbol{u}\}[x]$ での既約性の判定法，および可約な場合の分解法が問題となる．この例では，$F = (x^2 - u^3)^2 - u^7 = (x^2 - u^3 + xu^2 + \frac{1}{2}u^4 + \frac{1}{8}xu^3 + \frac{1}{8}u^5 + \cdots)(x^2 - u^3 - xu^2 + \frac{1}{2}u^4 - \frac{1}{8}xu^3 + \frac{1}{8}u^5 - \cdots)$ と分解できる．

Newton 多項式が重複因子を持つ場合，その因子の既約性判定法および分解法として，2 変数の場合，展開基底法と拡張 Hensel 構成を用いた方法が知られているが，多変数 (本稿では 3 変数以上のこと) の場合は方法がなかったため，新しいアルゴリズムを開発した．

多変数の拡張 Hensel 構成で得られる因子は，x と全次数変数 t に関しては多項式だが，従変数部分は有理式となることも，もう一つの問題である．これらの因子は $\overline{K}\{\boldsymbol{u}\}[x]$ を部分集合として含むある環に属しており，その環を $\overline{K}\{(\boldsymbol{u})\}[x]$ で表す：

$$\overline{K}\{(\boldsymbol{u})\} \stackrel{\mathrm{def}}{=} \left\{ \sum_{k=0}^{\infty}\left[\frac{N_k(\boldsymbol{u})}{D_k(\boldsymbol{u})}\right] \;\middle|\; \begin{array}{l} N_k(\boldsymbol{u}) \text{ と } D_k(\boldsymbol{u}) \text{ は } \mathrm{tdeg}(N_k) - \mathrm{tdeg}(D_k) = k \\ (k = 0, 1, 2, \cdots) \text{ なる } \boldsymbol{u} \text{ の同次多項式} \end{array} \right\}.$$

そこで，解析的因数分解の手順として，多変数においては，まず $\overline{K}\{(\boldsymbol{u})\}[x]$ での因数分解を求め，分母をキャンセルするように因子をかけあわせて (組合せは分母の特徴で決めることができる)，目標である $\overline{K}\{\boldsymbol{u}\}[x]$ での因数分解を得る戦略をとる．すなわち，$g_1(x, \boldsymbol{u}), \cdots, g_r(x, \boldsymbol{u}), g_{r+1}(x, \boldsymbol{u}), \cdots, g_{r+r'}(x, \boldsymbol{u})$ を $\overline{K}$ 上の既約多項式，$m_{r+1}, \cdots, m_{r+r'}$ を 2 以上の自然数とするとき，まず，

$$\begin{array}{lcccccccccc} F_{\mathrm{New}} & = & f_D(0) & x^{n_0} & g_1(x,\boldsymbol{u}) & \cdots & g_r(x,\boldsymbol{u}) & g_{r+1}(x,\boldsymbol{u})^{m_{r+1}} & \cdots & g_{r+r'}(x,\boldsymbol{u})^{m_{r+r'}} \\ & = & f_D(0) & F_0^{(0)} & F_1^{(0)} & \cdots & F_r^{(0)} & F_{r+1}^{(0)} & \cdots & F_{r+r'}^{(0)} \\ \text{拡張 Hensel 構成} \Downarrow & \vdots & \Downarrow & \Downarrow & \Downarrow & \cdots & \Downarrow & \Downarrow & \cdots & \Downarrow \\ F(x,\boldsymbol{u}) & = & f_D(\boldsymbol{u}) & F_0^{(\infty)} & F_1^{(\infty)} & \cdots & F_r^{(\infty)} & F_{r+1}^{(\infty)} & \cdots & F_{r+r'}^{(\infty)} \end{array}$$

と分解する．ただし，$n_0 = 1$ の場合は，x^{n_0} は $g_1(x, \boldsymbol{u}), \cdots, g_r(x, \boldsymbol{u})$ のどれかに含めればよく，$n_0 \geq 2$ の場合は，$F_0^{(\infty)}$ は再帰的に拡張 Hensel 構成を施して分解すればよい．$F_1^{(\infty)}, \cdots, F_r^{(\infty)}$ は $\overline{K}\{(\boldsymbol{u})\}[x]$ で既約である．したがって，問題は，$F_{r+1}^{(\infty)}, \cdots, F_{r+r'}^{(\infty)}$ の $\overline{K}\{(\boldsymbol{u})\}[x]$ での分解，すなわち，

$$F = \underbrace{g^m}_{F_{\mathrm{New}}} + \cdots (g \text{ は} \overline{K}[x, \boldsymbol{u}] \text{ の既約多項式}, m \geq 2) \text{ を} \overline{K}\{(\boldsymbol{u})\}[x] \text{ でどう因数分解するか?}$$

に帰着される．解析的因数分解の研究とは，つまるところ，この問題をいかに解決するかである．2 変数の場合には，2 つの方法が知られている．1 つは，Abhyankar[1, 2, 3, 4, 5] のアイデアをもとに Kuo[6] が考案し，McCallum[7] がより完全な形で実装した，展開基底法であり，g を新たな変数とみなして展開することで解決している．もう 1 つは，拡張 Hensel 構成を利用した Sasaki の方法 [10] で，分数べきを導入することで $g = x^{\hat{d}} - cu^{\hat{\delta}} = \prod_{i=1}^{\hat{d}}(x - c^{1/\hat{d}}e^{2i\pi\mathrm{i}/\hat{d}}u^{\hat{\delta}/\hat{d}})$，$\mathrm{i} = \sqrt{-1}$ のように互いに素な因子の積に分解し，これらを初期因子として拡張 Hensel 構成で分解し，共役性を利用して因子をかけあわせて解析的因子を求めている．これらの先行研究をもとに，筆者は，[11] で $g = \prod_{i=1}^{\hat{d}}(x - t^{\hat{\delta}/\hat{d}}\theta_i)$ と分解して拡張 Hensel 構成を利用 (θ_i は代数関数) して 3 変数以上に拡張した．さらに [12, 13] で，多変数用展開基底を提案した．

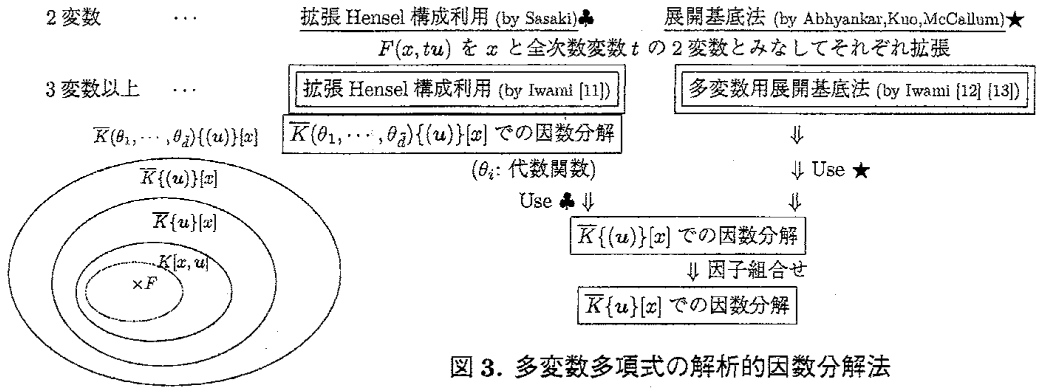


図 3. 多変数多項式の解析的因数分解法

拡張 Hensel 構成を利用した算法では，代数関数を導入することにより，$\overline{K}\{(\boldsymbol{u})\}[x]$ より大きな環である $\overline{K}(\theta_1,\cdots,\theta_{\tilde{d}})\{(\boldsymbol{u})\}[x]$ を経由する必要があるが，展開基底を用いた算法では，そのような大きな環を経由する必要がないことに注意されたい．

2 主係数が非特異な場合

まず，拡張 Hensel 構成を利用した方法について説明する．ここでは，重複既約成分 g を代数関数 $\theta_1,\cdots,\theta_{\tilde{d}}$ を導入することで互いに素な因子の積に分解し，それらを初期因子として拡張 Hensel 構成する．そして下図のように，共役な拡張 Hensel 因子をかけ合わせる．すると，根と係数の関係により代数関数が消え，$\overline{K}\{(\boldsymbol{u})\}[x]$ での因数分解を得る．この操作を再帰的に行う．

拡張 Hensel 構成を用いた $\overline{K}\{(\boldsymbol{u})\}[x]$ での因数分解法 $\boxed{\textbf{Iwami [11]}}$

$$
\begin{array}{rccc}
F_{\rm New} = g^m = & (x - t^{\hat{\delta}/\hat{d}}\theta_1)^m & \cdots & (x - t^{\hat{\delta}/\hat{d}}\theta_{\tilde{d}})^m \\
= & F_{\theta_1}^{(0)} & \cdots & F_{\theta_{\tilde{d}}}^{(0)} \\
\text{拡張 Hensel 構成} & \Downarrow & \cdots & \Downarrow \\
F = & F_{\theta_1}^{(\infty)} & \cdots & F_{\theta_{\tilde{d}}}^{(\infty)} \\
\text{Tschirnhausen変換 } T_x & \downarrow & \cdots & \downarrow \\
 & H_{\theta_1} & \cdots & H_{\theta_{\tilde{d}}} \\
\overline{K}(\theta_i)\{(\boldsymbol{u})\}[x] \text{ で再帰的に} & \Downarrow & \cdots & \Downarrow \\
\text{拡張 Hensel 構成} & H_{\theta_1 1}\cdots H_{\theta_1 \lambda} & \cdots & H_{\theta_{\tilde{d}} 1}\cdots H_{\theta_{\tilde{d}}\lambda} \\
T_x^{-1} & \downarrow\ \cdots\ \downarrow & \cdots & \downarrow\ \cdots\ \downarrow \\
F = & [T_x^{-1}\cdot H_{\theta_1 1}]\cdots[T_x^{-1}\cdot H_{\theta_1\lambda}] & \cdots & [T_x^{-1}\cdot H_{\theta_{\tilde{d}}1}]\cdots[T_x\cdot H_{\theta_{\tilde{d}}\lambda}]
\end{array}
$$

$$
\begin{array}{lclcccc}
F_{\theta_1}^{(\infty)} & = [T_x^{-1}\cdot H_{\theta_1}] & = & [T_x^{-1}\cdot H_{\theta_1 1}] & \cdots & [T_x^{-1}\cdot H_{\theta_1\lambda}] \\
\vdots & \quad\vdots & & \vdots & & \vdots \\
F_{\theta_{\tilde{d}}}^{(\infty)} & = [T_x^{-1}\cdot H_{\theta_{\tilde{d}}}] & = & [T_x^{-1}\cdot H_{\theta_{\tilde{d}}1}] & \cdots & [T_x^{-1}\cdot H_{\theta_{\tilde{d}}\lambda}] \\
 & & & \downarrow & & \downarrow \\
F(x,u) & & = & \hat{F}_1 & \cdots & \hat{F}_\lambda .
\end{array}
$$

$\hat{F}_i = \prod_{j=1}^{\tilde{d}}[T_x^{-1}\cdot H_{\theta_j i}]$ $(i=1,\cdots,\lambda)$ は $\overline{K}\{(\boldsymbol{u})\}[x]$ の既約因子

次に，多変数用展開基底法について説明する．ここでは，重複既約成分 $g(\stackrel{\rm def}{=} G_1)$ を新たな主変数とみなし，従変数の全次数変数 $t(\stackrel{\rm def}{=} G_{-1})$ と元の主変数 $x(\stackrel{\rm def}{=} G_0)$ を重みつき従変数とみなして与式を展開する．このとき，G_{-1} の重みを 1，$G_i (i \geq 2)$ の重み w_i を，G_i のべきを横軸にとったときの Newton 線の傾きの (-1) 倍で定めればよい．ここで得られた新たな Newton 多項式を，重みの差をうまく利用して pseudo form

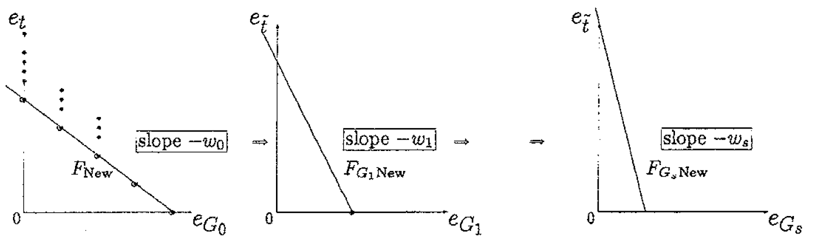
と呼ばれる形に変形し，$\overline{K}\{(\boldsymbol{u})\}$ 上，互いに素な因子の積に分解する．重複していて互いに素に分解できないときには，その重複既約成分を新たな主変数 G_2 とおき，それ以外の G_{-1}, G_0, G_1 を重みつき従変数とみなして展開し (G_2, G_1, G_0, G_{-1} の順で割ることで一意表現の $\mathcal{G}$-adic expansion が得られる)，新たな Newton 多項式を計算する．初期因子が重複している限りこの主変数の置きかえ (軸変換) が行われる．lifting には，分母に元の主変数 x があらわれないように変形した補間式，practical interpolation polynomial ([12] 参照) を用いる．

展開基底を用いた $\overline{K}\{(\boldsymbol{u})\}[x]$ での因数分解法 **Iwami [12]**

展開基底	:	$G_{-1} = t,$	$G_0 = x,$		$G_1 = g,$		$\cdots$		G_s
重み	:	1 (初期値)	w_0	$<$	w_1	$<$	$\cdots$	$<$	w_s

$\mathcal{G}$-adic expansion $F = \Sigma_{e_s=0}^{\tilde{m}} c(\boldsymbol{u}) G_{-1}^{e_{-1}} G_0^{e_0} G_1^{e_1} \cdots G_s^{e_s}$, $c(\boldsymbol{u}) \in \overline{K}\{(\boldsymbol{u})\}$, $\tilde{m} = \deg_x(F)/\deg_x(G_s)$,

$G_i \mapsto \tilde{t}^{w_i} G_i$ $(i = -1, 0, \cdots, s-1)$.



3 主係数が特異な場合

2 変数の場合，主係数特異な F は，$F = F_1 F_2$ (F_1 の主係数は非特異，F_2 は $\overline{K}\{(\boldsymbol{u})\}[x]$ の単元) と分解できる．解析的因数分解では単元の分解は考えないので，主係数非特異な因子の解析的因数分解に帰着されるので，問題とはならない．

多変数で問題となる主係数特異，すなわち $f_D(\boldsymbol{0}) = 0$ の場合の分解法として，拡張 Hensel 構成を用いた算法である [11] の後半，および，多変数用展開基底を用いた算法である [13] がある．以下，新しい成果である後者ついて述べる．この算法では，“拡張 Hensel 構成における Newton 線の傾き” と “展開基底の重み” を対応させて考えることで，結果として拡張 Hensel 構成と展開基底のテクニックの融合が実現している．さらに，主係数非特異な場合にも利用できる，統一的な算法となっている．

一般性を失うことなく，初期処理として拡張 Hensel 構成を施したあとは，定理 1 の仮定にある $F(x, \boldsymbol{u})$ を考えればよい．

定理 1

$F(x, t\boldsymbol{u})$ は $F_{\mathrm{New}} = f_D(\boldsymbol{u}) x^D + \cdots + f_0(\boldsymbol{u}) = c(\boldsymbol{u}) g^m$ ($c(\boldsymbol{u}) \in \overline{K}[\boldsymbol{u}]$, $m \geq 2$, g は $\overline{K}[x, \boldsymbol{u}]$ で既約) かつ $\mathrm{ord}_t f_D(\boldsymbol{u}) \overset{\mathrm{def}}{=} \nu \gneq 0$ (i.e. $f_D(\boldsymbol{0}) = 0$) とする．このとき，Newton 線の傾きを $\hat{\lambda}$，F の展開基底を $\mathcal{G} = (G_{-1}(= t), G_0(= x), G_1(= g))$，重みを $\mathcal{W} = (w_{-1}(= 1), w_0(= -\hat{\lambda}), w_1)$，$F(G_{-1}, G_0, G_1)$ を F の $\mathcal{G}$-adic expansion とする．このとき，

$$\hat{F}(G_1, G_0, G_{-1}, \tilde{t}) \overset{\mathrm{def}}{=} F(\tilde{t}^{w_{-1}} G_{-1}, \tilde{t}^{w_0} G_0, \tilde{t}^{w_1} G_1) / \tilde{t}^{\nu + D w_0}$$

の各項に対応する点を $(e_{G_1}, e_{\tilde{t}})$-平面 (ここで横軸は G_1 のべき，縦軸は $\tilde{t}$ のべきをあらわす) にプロットすると，Newton 線 $\mathcal{L}_{G_1}$ 上の点は真下に移動して横軸上に乗り，このとき横軸成分が最大になる点は $(m, 0)$

である．また，このときの Newton 多項式 $\hat{F}_{G_1\mathrm{New}}$ と lifting に用いるイデアル $\hat{I}_k$ は次となる．

$$\hat{F}_{G_1\mathrm{New}} = \hat{F}(G_{-1}, G_0, G_1, \tilde{t}=0), \quad \hat{I}_k = \left\langle \tilde{t}^{k/\hat{m}} \right\rangle,\ k=1,2,3,\cdots.$$

ただし，|Newton 線 $\mathcal{L}_{G_1}$ の傾き | $= \hat{n}/\hat{m}$,（$\hat{m}$と$\hat{n}$は互いに素な正の整数）とする．

証明 [9] での変換 $\hat{F}(x,\boldsymbol{u},t) \stackrel{\mathrm{def}}{=} F(t^{-\hat{\lambda}}x, t\boldsymbol{u})/t^{\nu-D\hat{\lambda}}$ により，Newton 線上の全ての項は真下に移り，横軸上にのる．ここで，(D,ν) は $(D,0)$ に移動し，かつ横軸成分が D より大きい点は存在しない．以下，この変換を，

$$(\text{展開基底 } G_i \text{の重み } w_i) \stackrel{\mathrm{def}}{=} (-1)\times(\text{Newton 線 } \mathcal{L}_{G_i} \text{の傾き})$$

と定義することで，多変数用展開基底用に拡張する．

仮定により，Newton 多項式 $F_{\mathrm{New}} = \hat{F}(x,\boldsymbol{u},t=0) = c(\boldsymbol{u})g^m$ は重複していて $\overline{K}\{\boldsymbol{u}\}[x]$ で互いに素な，単元でない因子の積に分解することができないため，多変数用展開基底とその重みをそれぞれ $\mathcal{G} = (G_{-1}, G_0, G_1) = (t, x, g), \mathcal{W} = (w_{-1}, w_0) = (1, -\hat{\lambda})$ と設定する．与式 $F(x, t\boldsymbol{u})$ を G_1, G_0, G_{-1} の順に割ることで一意的な表現である $F(x, t\boldsymbol{u})$ の $\mathcal{G}$-adic expansion $F(G_{-1}, G_0, G_1) = \Sigma_{e_1=0}^{m} c_{(e_{-1},e_0,e_1)}(\boldsymbol{u}) G_{-1}^{e_{-1}} G_0^{e_0} G_1^{e_1}$, $c_{e_{-1},e_0,e_1}(\boldsymbol{u}) \in \overline{K}\{(\boldsymbol{u})\}$ を計算し，$F(\tilde{t}^{w_{-1}}G_{-1}, \tilde{t}^{w_0}G_0, G_1)$ の各項を $(e_{G_1}, e_{\tilde{t}})$-平面にプロットすると，G_1 を主変数, G_0, G_{-1} を従変数とみなしたときの新たな Newton 多項式を得る．

主係数が特異な場合には，（展開基底 G_1の重み w_1）$\stackrel{\mathrm{def}}{=} (-1)\times$（Newton 線 $\mathcal{L}_{G_1}$の傾き）を用いることで $F(\tilde{t}^{w_{-1}}G_{-1}, \tilde{t}^{w_0}G_0, \tilde{t}^{w_1}G_1)$ と変換して Newton 線を水平にすることができ，さらに $\tilde{t}^{\nu+Dw_0}$ で割ることで横軸に重ね合わせることができる．また，$F_{\mathrm{New.}} = c(\boldsymbol{u})g^m = c(\boldsymbol{u})G_1^m$ であり，かつ，得られた Newton 線は横軸上にあることから，横軸成分が最大になる点は $(m, 0)$ である．

また，$\hat{F}(G_{-1}, G_0, G_1, \tilde{t}) = F(\tilde{t}^{w_{-1}}G_{-1}, \tilde{t}^{w_0}G_0, \tilde{t}^{w_1}G_1)/\tilde{t}^{\nu+Dw_0}$ に $\tilde{t}=0$ を代入すると，横軸上の点に対応する項全ての和，すなわち，Newton 多項式 $F_{G_1\mathrm{New}}$ が計算できる．このとき lifting は $1/\hat{m}$ づつ水平に $e_{\tilde{t}}$ 方向に実行すればよいので，用いるイデアルは $\hat{I}_k = \langle \tilde{t}^{k/\hat{m}} \rangle$, $k=1,2,3,\cdots$ となる．∎

この変換により，$\tilde{t}=0$ を代入して得られる Newton 多項式 $\hat{F}_{G_1\mathrm{New}} = \hat{F}(G_1, G_0, G_{-1}, \tilde{t}=0)$ で主係数が消えないことに注意されたい．また，Newton 線を水平に変換すると，取り扱いやすくなる．なぜなら，$\tilde{t}=0$ を代入するだけで Newton 多項式が計算でき，さらに，lifting する際のイデアルが $\hat{I} = (\tilde{t}^{k/\hat{m}})$, $k=1,2,3,\cdots$ とシンプルだからである．したがって，展開基底 $\mathcal{G} = (G_{-1}, G_0, G_1, \cdots, G_s)$ に対して Newton 線を水平に変換するために，次のような一般化を行う．

定理 2
F の多変数用展開基底を $\mathcal{G} = (G_{-1}, G_0, G_1, \cdots, G_s)$，その重みを $\mathcal{W} = (w_{-1}, w_0, w_1, \cdots, w_s)$ (w_i は $\mathcal{L}_{G_i\mathrm{New}}$ の傾きの(-1)倍で定義される）とする．$F(G_{-1}, G_0, G_1, \cdots, G_s)$ を F の $\mathcal{G}$-adic expansion とする．このとき，主係数が特異であれ非特異であれ，

$$\hat{F}(G_{-1}, G_0, G_1, \cdots, G_s, \tilde{t}) \stackrel{\mathrm{def}}{=} F(\tilde{t}^{w_{-1}}G_{-1}, \tilde{t}^{w_0}G_0, \tilde{t}^{w_1}G_1, \cdots, \tilde{t}^{w_s}G_s)/\tilde{t}^{\alpha},$$
$$\alpha = \mathrm{ord}_{\tilde{t}} F(\tilde{t}^{w_{-1}}G_{-1}, \cdots, \tilde{t}^{w_{s-1}}G_{s-1}, \tilde{t}^{w_s}G_s)$$

の各項に対応する点を $(e_{G_s}, e_{\tilde{t}})$-平面にプロットすると，Newton 線 $\mathcal{L}_{G_s}$ は水平となって横軸上に移る．また，$\tilde{t}=0$ を代入したとき主係数が消えない．このときの Newton 多項式 $\hat{F}_{G_s\mathrm{New}}$ と lifting に用いるイデアル $\hat{I}_k$ は次となる．

$$\hat{F}_{G_s\mathrm{New}} = \hat{F}(G_{-1}, G_0, G_1, \cdots, G_s, \tilde{t}=0), \quad \hat{I}_k = \left\langle \tilde{t}^{k/\hat{m}} \right\rangle,\ k=1,2,3,\cdots.$$

ただし，|Newton 線 $\mathcal{L}_{G_s}$ の傾き | $= \hat{n}/\hat{m}$,（$\hat{m}$と$\hat{n}$は互いに素な正の整数）とする．

証明 展開基底が生成されるのに伴って，横軸が $e_{G_0} \to \cdots \to e_{G_s}$ と置き換わる．このとき，各ステップ毎に，縦軸の $e_{\tilde{t}}$ の値は，$G_{-1}, \cdots, G_{s-1}$ の重みつき全次数変数のべきとして足し込められていく．

さらに G_s を $\tilde{t}^{w_{G_s}} G_s$ とすることで $\mathcal{L}_{G_s}$ は水平に変換され，$\tilde{t}^{\mathrm{ord}_{\tilde{t}} F(\tilde{t}^{w_s} G_s, \cdots, \tilde{t}^{w_{-1}} G_{-1})}$ で割ることで，$\mathcal{L}_{G_s}$ 上の全ての項を真下に移動させ，横軸上にのせることができる．$\tilde{t} = 0$ で主係数が消えないこと，$\hat{F}_{G_s\mathrm{New}} = \hat{F}(G_{-1}, G_0, G_1, \cdots, G_s, \tilde{t} = 0)$, $\hat{I}_k = \langle \tilde{t}^{k/\hat{m}} \rangle$, $k = 1, 2, 3, \cdots$. は定理 1 と同様に示される． ∎

アルゴリズム 1 (主係数特異な場合を含む多変数用展開基底法による因数分解アルゴリズム)

INPUT : $F(x, \boldsymbol{u}) \in \overline{K}\{(\boldsymbol{u})\}[x]$ *s.t.* $F_{\mathrm{New}} = c(\boldsymbol{u}) g^m$ ($m \geq 2$, g は $\overline{K}[x, \boldsymbol{u}]$ で既約).
OUTPUT : $\overline{K}\{(\boldsymbol{u})\}[x]$ での既約因子.

1. 展開基底 $\mathcal{G} = (G_{-1}(=t), G_0(=x), G_1(=g), \cdots, G_s)$ とその重み $\mathcal{W} = (w_{-1}(=1), w_0, \cdots, w_{s-1})$ を計算する．そして F を $G_s, \cdots, G_1, G_0, G_{-1}$ の順で割ることで，次のように $\mathcal{G}$-adic expansion する．

$$F(G_{-1}, G_0, \cdots, G_s) = \Sigma c_{(e_{-1}, e_0, \cdots, e_s)}(\boldsymbol{u}) G_{-1}^{e_0} G_0^{e_0} \cdots G_s^{e_s}$$

2. $F(\tilde{t}^{w_{-1}} G_{-1}, \tilde{t}^{w_0} G_0, \cdots, \tilde{t}^{w_{s-1}} G_{s-1}, G_s)$ の各項を $(e_{G_s}, e_{\tilde{t}})$-平面上にプロットし，G_s の重み w_s を次で定義する．

$$(G_s \text{の重み } w_s) \stackrel{\mathrm{def}}{=} (-1) \times (\text{Newton 線 } \mathcal{L}_{G_s} \text{の傾き})$$

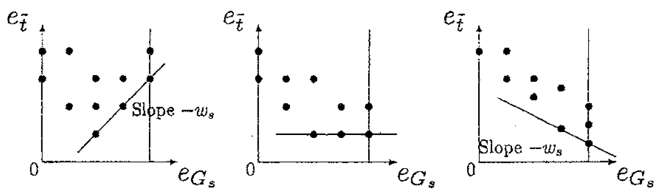
3. $\hat{F}(G_{-1}, \cdots, G_s, \tilde{t}) = F(\tilde{t}^{w_{-1}} G_{-1}, \cdots, \tilde{t}^{w_s} G_s) / \tilde{t}^{\mathrm{ord}_{\tilde{t}} F(\tilde{t}^{w_{-1}} G_{-1}, \cdots, \tilde{t}^{w_s} G_s)}$ を計算する．

4. $\hat{F}_{G_s\mathrm{New}} = \hat{F}(G_s, \cdots, G_{-1}, \tilde{t} = 0)$ を *pseudo form* に書き換え，$\overline{K}\{(\boldsymbol{u})\}$ 上因数分解する．

   - 互いに素な因子の積に分解できない場合，重複度が 1 なら既約．重複度が 2 以上なら，重複既約成分を G_{s+1} とおいて展開基底 $\mathcal{G}$ に追加し，**1.**($s \leftarrow s+1$) へすすむ．

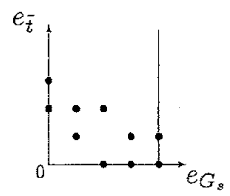
   - 互いに素な因子の積に分解できる場合，それらを初期因子として イデアル $\hat{I}_k = \langle \tilde{t}^{k/\hat{m}} \rangle$, $k = 1, 2, 3, \cdots$. で lifting する．このとき用いる補間式は，分母に元の主変数 x があらわれないように変形したものを用いる (詳細は [12, 13] を参照されたい).

Newton dots for $F(\tilde{t}^{w_{-1}} G_{-1}, \cdots, \tilde{t}^{w_{s-1}} G_{s-1}, G_s)$



$$\Longrightarrow \; F(\tilde{t}^{w_{-1}} G_{-1}, \cdots, \tilde{t}^{w_{s-1}} G_{s-1}, \tilde{t}^{w_s} G_s) / \tilde{t}^{\alpha}$$

$$\alpha = \mathrm{ord}_{\tilde{t}} F(\tilde{t}^{w_{-1}} G_{-1}, \cdots, \tilde{t}^{w_{s-1}} G_{s-1}, \tilde{t}^{w_s} G_s)$$



Example

$$F(x,u_1,u_2) \stackrel{\mathrm{def}}{=} \left((u_1+2u_2)\left(\underline{u_2^3\,x^2-(u_1+u_2)}\right)^2-u_1^7x^2-u_1^9\right)\left(\left(\underline{u_2^3\,x^2-(u_1+u_2)}\right)^2-(u_1+u_2)^3u_2\right).$$

$F(x,u_1,u_2)$ は，本稿で述べた主係数特異な場合を含む多変数用展開基底アルゴリズムにより，$\overline{K}\{\boldsymbol{u}\}[x]$ で次のように因数分解することができる．

$$\begin{aligned}
&F(x,u_1,u_2) = \left((u_1+2u_2)\left(\underline{u_2^3\,x^2-(u_1+u_2)}\right)^2-u_1^7x^2-u_1^9\right)\\
&\times\left(\underline{u_2^3\,x^2-(u_1+u_2)}-u_2^2(u_1+u_2)x+\tfrac{1}{2}u_2(u_1+u_2)^2-\tfrac{1}{8}u_2^2(u_1+u_2)^3-\tfrac{1}{8}u_2^3(u_1+u_2)^2x+\cdots\right)\\
&\times\left(\underline{u_2^3\,x^2-(u_1+u_2)}+u_2^2(u_1+u_2)x+\tfrac{1}{2}u_2(u_1+u_2)^2+\tfrac{1}{8}u_2^2(u_1+u_2)^3+\tfrac{1}{8}u_2^3(u_1+u_2)^2x+\cdots\right).
\end{aligned}$$

まず，$F(x,t\boldsymbol{u})$ の各項に対応する点を (e_x,e_t)-平面にプロットしたものがFig.A-1である．変換 $F(\tilde{t}^{-1}x,\tilde{t}\boldsymbol{u})/\tilde{t}^5$ を施した後の $(e_x,e_{\tilde{t}})$-平面の各項に対応する点は Fig.A-2のようになる．このとき，ニュートン多項式 F_{New} は，$F_{\mathrm{New}}=(u_1+2u_2)t\left(\underline{u_2^3\,t^3x^2-(u_1+u_2)t}\right)^4$ ゆえ，$\overline{K}$ 上，単元でない互いに素な既約多項式に分解できず，かつ主係数が展開点 $u_1=u_2=0$ でゼロになる．ここで，展開基底を $\mathcal{G}=(G_{-1},G_0,G_1)=(t,\,x,\,u_2^3t^3x^2-(u_1+u_2)t)$ とおく．$\mathcal{L}_{\mathrm{New}}$ の傾きが 1 なので，重みは $\mathcal{W}=(w_{-1},w_0)=(1,-1)$ と定められる．F を G_1,G_0,G_{-1} の順で割ることで一意表現の $\mathcal{G}$-adic expansion $F=\Sigma_{e_1=0}^{m}c_{(e_{-1},e_0,e_1)}(\boldsymbol{u})G_{-1}^{e_{-1}}G_0^{e_0}G_1^{e_1}$，$c_{(e_{-1},e_0,e_1)}(\boldsymbol{u})\in\overline{K}\{(\boldsymbol{u})\}$ で表す．ここで，$\tilde{F}(G_1,\tilde{t}^{-1}G_0,\tilde{t}^1G_{-1})$ を $(e_{G_1},e_{\tilde{t}})$-平面 にプロットしたときの $\mathcal{L}_{G_1\mathrm{New}}$ の傾きが -2 なので，G_1 の重みが $w_1=2$ と定められる．(FigB-1 参照)．したがって，$\hat{F}(G_{-1},G_0,G_1,\tilde{t})=F(\tilde{t}^1G_{-1},\tilde{t}^{-1}G_0,\tilde{t}^2G_1)/\tilde{t}^9$ なる変換を施す (Fig B-2 参照)．

以上により，$\hat{F}_{G_1\mathrm{New}}=\hat{F}(G_{-1},G_0,G_1,\tilde{t}=0)=(G_1^2-u_2(u_1+u_2)^3G_{-1}^4)\left((u_1+2u_2)G_{-1}G_1^2-\frac{u_1^7}{u_2^3}(u_1+u_2)G_{-1}^5\right)$ のように，単元でない互いに素な因子の積に分解することができた．

展開基底 G_1 の定め方より，$(\tilde{t}^{w_1}G_1)=u_2^3(\tilde{t}^{w_{-1}}G_{-1})^3(\tilde{t}^{w_0}G_0)^2-(u_1+u_2)(\tilde{t}^{w_{-1}}G_{-1})$ であるから，関係式 $(u_1+u_2)G_{-1}=u_2^3G_{-1}^3G_0^2-\tilde{t}G_1$ を得る．各項の重みは次のとおり．

$$\begin{array}{rcccccc}
 & (u_1+u_2)G_{-1} & = & u_2^3G_{-1}^3G_0^2 & - & \tilde{t}G_1 \\
\text{Weights} & 1 & & 1 & & 2
\end{array}$$

したがって，$\hat{F}_{G_1\mathrm{New}}$ を，$(u_1+u_2)G_{-1}\to u_2^3G_{-1}^3G_0^2$ とすることで，同じ重み 1 をもつ別表現にして，次のように pseudo form F^* に書き換えることができる．

$$\begin{aligned}
F^* &= (G_1^2-u_2^4(u_1+u_2)^2G_{-1}^6G_0^2)\left((u_1+2u_2)G_{-1}G_1^2-u_1^7G_{-1}^7G_0^2\right)\\
&= (G_1+u_2^2(u_1+u_2)G_{-1}^3G_0)(G_1-u_2^2(u_1+u_2)G_{-1}^3G_0)\left((u_1+2u_2)G_{-1}G_1^2-u_1^7G_{-1}^7G_0^2\right)
\end{aligned}$$

したがって，互いに素な 3 つの初期因子 $u_2^3x^2-(u_1+u_2)+u_2^2(u_1+u_2)x, u_2^3x^2-(u_1+u_2)-u_2^2(u_1+u_2)x,$ and $(u_1+2u_2)\left(u_2^3x^2-(u_1+u_2)\right)^2-u_1^7x^2$. を得ることができた．lifting することで，次のような F の因子を求めることができる．

$$\begin{aligned}
F &= \left(u_2^3\,x^2-(u_1+u_2)+u_2^2(u_1+u_2)x+\tfrac{1}{2}u_2(u_1+u_2)^2+\tfrac{1}{8}u_2^2(u_1+u_2)^3+\cdots\right)\\
&\times\left(u_2^3\,x^2-(u_1+u_2)-u_2^2(u_1+u_2)x+\tfrac{1}{2}u_2(u_1+u_2)^2-\tfrac{1}{8}u_2^2(u_1+u_2)^3-\cdots\right)\\
&\times\left((u_1+2u_2)\left(u_2^3\,x^2-(u_1+u_2)\right)^2-u_1^7x^2-u_1^9\right).
\end{aligned}$$

$F(x, tu_1, \cdots, tu_\ell)$ Plot (e_x, e_t) slope $1 \Rightarrow w_0 = -1$ | $F(\tilde{t}^{-1}x, \tilde{t}u_1, \cdots, \tilde{t}u_\ell)/\tilde{t}^5$ Plot $(e_x, e_{\tilde{t}})$ | $F(\tilde{t}^1 G_{-1}, \tilde{t}^{-1}G_0, G_1)$ Plot $(e_{G_1}, e_{\tilde{t}})$ slope $-2 \Rightarrow w_1 = 2$ | $F(\tilde{t}^1 G_{-1}, \tilde{t}^{-1}G_0, \tilde{t}^2 G_1)/\tilde{t}^9$ Plot $(e_{G_1}, e_{\tilde{t}})$

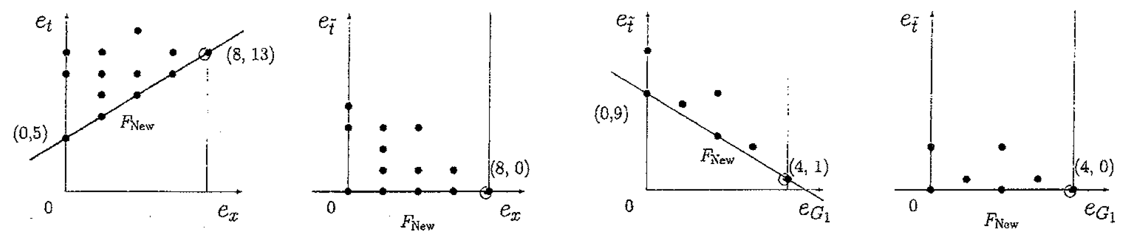


Fig.A-1　Fig.A-2　Fig.B-1　Fig.B-2

4　まとめ

3 章で，主係数が特異な場合を含む，解析的因数分解のための多変数用展開基底 [13] について述べた．ここでは，[9] で用いている変換を多変数用展開基底に適用することで，主係数が特異であれ非特異であれ，統一的に計算できることが示されている．この算法は，“展開基底の重み” と “Newton 線の傾き” を対応づけることで実現された．2 変数の展開基底の重みは正の値しか取り得なかったのに対し，多変数用展開基底の重みは負，0，正 (このとき Newton 線の傾きはそれぞれ正，0，負) の値を取り得ることに注意されたい．よって，この統一的算法は多変数用展開基底と拡張 Hensel 構成，両者のテクニックを融合させたものとなっている．

$\overline{K}[x, \boldsymbol{u}]$ での因数分解に関して，[9] では，Newton 多項式が無平方なものに限定されていたが，[11, 12, 13] を用いると，Newton 多項式が無平方でない場合でも計算できる．なぜなら，$\overline{K}[x, \boldsymbol{u}] \subset \overline{K}\{\boldsymbol{u}\}[x] \subset \overline{K}\{(\boldsymbol{u})\}[x]$ より，解析的既約因子をかけあわせることで $\overline{K}[x, \boldsymbol{u}]$ の既約因子を得ることができるからである．

参 考 文 献

[1] S. S. Abhyankar: Local Analytic geometry. Academic Press, New York (1964).

[2] S. S. Abhyankar: What is the difference between a parabola and a hyperbola? Math. Intelligencer 10 (1988) pp.37–43.

[3] S. S. Abhyankar: Irreducibility Criterion for Germs of Analytic Functions of Two Complex Variables. Advances in Math., 74 (1989) pp. 190–257.

[4] S. S. Abhyankar and T. T. Moh: Newton-Puiseux expansion and generalized Tschirnhausen transformation II. J. reine und angew. Math. 261, (1973) pp.29–54.

[5] S. S. Abhyankar: *Algebraic Geometry for Scientists and Engineers.* Number 35 in Mathematical Surveys and Monographs. Providence, RI: Amarican Mathematical Society (1990).

[6] T. C. Kuo: Generalized Newton-Puiseux Theory and Hensel's Lemma in $C[[x, y]]$. Can. J. Math., Vol.XLI, No. 6 (1989) pp.1101–1116.

[7] S. McCallum: On Testing a Bivariate Polynomial for Analytic Reducibility. J. Symb. Comput. 24 (1997) pp.509–535.

[8] T. Sasaki and F. Kako: Solving Multivariate Algebraic Equation by Hensel Construction. Japan J. Indus. Appl. Math., 16 (1999) pp.257–285.

[9] T. Sasaki and D. Inaba: Hensel Construction of $F(x, u_1, \ldots, u_l)$, $l \geq 2$, at a Singular Point and Its Applications. SIGSAM Bulletin, Vol. 34 (2000) pp.9–17 .

[10] T. Sasaki: Properties of Extended Hensel Factors and Application to Approximate Factorization. Preprint (2000).

[11] M. Iwami: Analytic Factorization of the Multivariate Polynomial. Proceedings of the Sixth International Workshop on Computer Algebra in Scientific Computing (CASC2003), Institut für Informatik, Technische Universität München (2003), pp.213–225.

[12] M. Iwami: Extension of Expansion Base Algorithm to Multivariate Analytic Factorization. Proceedings of the Seventh International Workshop on Computer Algebra in Scientific Computing (CASC2004), Institut für Informatik, Technische Universität München (2004), pp.269–281.

[13] M. Iwami: Extension of Expansion Base Algorithm to Multivariate Analytic Factorization including the Case of Singular Leading Coefficient. (submitted)